NAVMC 2927
POS
9 Mar 98

FOREWORD

1. PURPOSE

    NAVMC 2927, ANTITERRORISM/FORCE PROTECTION CAMPAIGN PLAN,
establishes a baseline overview of the Marine Corps approach to
force protection. The Plan clarifies the issue of force
protection in regards to antiterrorism and provides commanders
with a source document upon which to institutionalize local
programs.

2. FREQUENCY

    This Manual will be revised biannually.

3. EFFECTIVE DATE

    This Manual is effective upon signature.

4. Recommendations for improving this Manual are invited and
should be submitted in writing to the Commandant of the Marine
Corps (POS).

5. RESERVE APPLICABILITY

    This Manual is applicable to the Marine Corps Reserve.

6. CERTIFICATION

    Reviewed and approved this date.

R. I. NEAL
Assistant Commandant
of the Marine Corps

DISTRIBUTION: PCN 10010361700

DISTRIBUTION STATEMENT A: Approved for public release;
                           distribution is unlimited

LOCATOR SHEET

Subj: <u>NAVMC 2927, ANTITERRORISM/FORCE PROTECTION CAMPAIGN PLAN</u>

Location: _____

   (Indicate location(s) of copy(ies) of this Manual.)

ANTITERRORISM/FORCE PROTECTION CAMPAIGN PLAN

RECORD OF CHANGES

Log completed change action as indicated.

Change Number	Date of Change	Date Received	Date Entered	Signature of Person Entering Change

ANTITERRORISM/FORCE PROTECTION CAMPAIGN PLAN

TABLE OF CONTENTS

INTRODUCTION

CHAPTER 1

INTELLIGENCE

CHAPTER 2

TRAINING AND EDUCATION

ANTITERRORISM/FORCE PROTECTION CAMPAIGN PLAN

TABLE OF CONTENTS   (contd)

CHAPTER 3

OPERATIONS

CHAPTER 4

RESOURCES

CHAPTER 5

COMMANDER'S RESPONSIBILITY

ANTITERRORISM/FORCE PROTECTION CAMPAIGN PLAN

TABLE OF CONTENTS (contd)

APPENDICES

V

ANTITERRORISM/FORCE PROTECTION CAMPAIGN PLAN

INTRODUCTION

0001. <u>PURPOSE</u> To provide an overview of the Marine Corps'
approach to antiterrorism/force protection and outline supporting
functions. To clarify the issue of force protection in regards
to antiterrorism and provide commanders with a source document
upon which to institutionalize local programs.

0002. <u>BACKGROUND</u>

1. <u>Commander's Intent</u>

    a. The complexion of our strategic operating environment has
changed considerably during the course of the last few years.
The end of the Cold War signaled a shift in threat focus from one
centering on an organized adversary to one characterized by
uncertainty. With this shift, our national strategy was
reoriented from one based on deterrence to one centered on
engagement and enlargement. What this has meant for the Marine
Corps is increasing importance on the utility of the Naval
Expeditionary Forces in meeting national strategic goals through
continued forward presence and enhanced power projection. Given
our continued forward presence, Marines and sailors will continue
to operate on the "tip of the spear1" and often in harm's way.

    b. The reemergence of an old adversary, the terrorist,
threatens the welfare of our troops and our ability to
successfully execute our missions. Those who recall Marine Corps
history know that the terrorist is not a new enemy. We faced
this enemy in Beirut in the 1980's. Recent terrorist events,
such as the release of sarin gas into the Tokyo subway system and
the bombings of the World Trade Center, U.S. facilities in the
Middle East, and Centennial Park during the Atlanta Olympic
Games, attest to the fact that our personnel are likely to be
targets of indiscriminate terrorist attacks in the future, both
at home and abroad.

    c. For Marines, force protection is nothing new. We have
long prided ourselves on taking care of our Marines and are
keenly aware that the security of personnel and equipment is an
inherent responsibility of the commander. Those in leadership
positions, regardless of rank, have a responsibility to ensure
that our forces are properly prepared to meet, counter, and

survive the terrorist threat. This Campaign Plan clarifies our objectives and provides guidance that will improve our ability to adequately protect our forces as we enter the 21st Century.

2. <u>Situation Overview</u>

    a. The potential for terrorists to strike against our military personnel is a well documented fact and one that is embedded in the history of our Corps. Most Marines vividly recall the terrorist bombing of the Marine compound in Beirut, Lebanon as well as the kidnapping and execution of Colonel William R. Higgins at the hands of terrorists. These are two of the more recent terrorist incidents that were directed specifically at members of our Corps. There have been, however, similar attacks directed toward American military personnel. Between 1972 and 1995, DOD military personnel and facilities have been targeted by terrorist factions on 405 separate occasions. The following is a representative sample of some of these incidents and is provided to highlight the fact that the threat is real and that it can happen to our personnel:

> * May 1978: Two separate bombings were directed at facilities housing U.S. military personnel and their family members, one at the U.S. Air Force transient quarters in Ankara, Turkey, the other at the U.S. Army hotel in Wiesbaden, Germany;
> * May 1979: The Marine Security Guard residence in Bogota, Colombia was bombed causing extensive damage and wounding four U.S. Marines;
> * June 1979: The Red Army Faction attempted to assassinate General Alexander Haig, Supreme Allied Commander, NATO. General Haig's vehicle narrowly escaped the bombing. Two guards were wounded;
> * December 1979: Two sailors were killed and 10 others injured when Puerto Rican terrorists ambushed the school bus in which they were riding;
> * March 1980: Members of the terrorist group Macheteros fired on a U.S. Navy bus in Puerto Rico killing two;
> * January 1981: Terrorists belonging to Macheteros destroyed eight aircraft and damaged two others in a carefully executed multiple bombing attack on the Puerto Rican Air National Guard. Damage exceeded $40 million;

* March 1981: Three Marines were wounded in a rocket attack on an embassy vehicle in San Jose, Costa Rica;
* December 1981: Red Brigade members kidnapped U.S. Army Brigadier General James Dozier from his home in Verona, Italy and held him captive for 42 days until he was freed by Italian counter terrorist forces;
* May 1982: Macheteros terrorists killed one U.S. sailor and injured three in an ambush outside a nightclub in San Juan, Puerto Rico;
* April 1983: Hizballah members launched a suicide bomb against the U.S. Embassy in Beirut, Lebanon killing 49 and wounding 120;
* October 1983: Suicidal terrorists from the Islamic Jihad drove two explosive laden trucks into the U.S. and French military barracks in Beirut claiming the lives of 241 service members and 46 French military personnel;
* August 1985: Red Army Faction detonated a car bomb at Rhein Main Air Force Base, Germany killing two and injuring 17. The night before the attack, the terrorists killed an off-duty U.S. serviceman and used his military identification card to gain access to the base;
* February 1988: Hizballah members kidnapped U.N Military Observer LtCol William R. Higgins, USMC. In July 1989, the terrorists broadcasted a videotape of his remains. LtCol Higgins' remains were returned to the U.S. in 1991;
* April 1988: Japanese Red Army members were held responsible for the bombing of a U.S. Servicemen's Club in Naples, Italy that killed five people. The bombing coincided with the anniversary of the U.S. raid on Libya in 1986;
* May 1990: A U.S. Marine Gunnery Sergeant was slain in a nighttime ambush by urban terrorists of the CPP/NPA outside Olongapo, Philippines;
* January 1991: Two U.S. servicemen were executed after their helicopter was downed by Farabundo Marti National Liberation Front (FMLN) militants in San Miguel, El Salvador;
* March 1991: A U.S. Air Force Sergeant was killed by a remote controlled bomb detonated at the

entrance of his apartment in Athens, Greece.
The revolutionary organization 17 November claimed
the attack was in response to the genocide of
13,000 Iraqis;

* December 1992: An explosion at the Gold Mihor Hotel
in Aden, Yemen killed a foreign diplomat and injured
his wife; about 100 U.S. servicemen participating in
Operation Restore Hope had been staying in Aden
since mid-December;

* September 1993: A U.N. truck carrying twelve tons
of medical supplies was destroyed by a bomb while
traveling near Irbil, Iraq wounding 13;

* September 1995: A rocket-propelled grenade was
fired at the U.S. Embassy in Moscow; authorities
suspect the attack was in retaliation for U.S.
participation in NATO airstrikes against Bosnia Serb
targets;

* November 1995: A car bomb exploded in a parking lot
at the Office of the Program Manager/Saudi Arabian
National Guard (OPM/SANG) in Riyadh, Saudi Arabia
killing seven and wounding 42;

* June 1996: Terrorists launched a truck bomb attack
against Khobar Towers, a contracted housing facility
near Dhahran, Saudi Arabia killing 19 servicemen and
injuring hundreds more.

    b. The preceding summations attest to the fact that U.S.
military personnel have been, and are likely to continue to be,
subject to indiscriminate terrorist attacks worldwide. The
targets of these attacks had one thing in common -- they were
all DOD-affiliated personnel who were regarded by the terrorist
as a symbol of America.

3. <u>What is "Force Protection"</u>

    a. A formal definition for force protection is found in
Joint Publication 5-03.2 which describes force protection as a
security program designed to protect military personnel, civilian
employees, family members, facilities, and equipment in all
locations and situations. Force protection is accomplished
through a systematic approach which integrates the planning and
application of combating terrorism, physical security, operations
security (OPSEC), and personal protective measures, supported by
intelligence, counterintelligence, and other security programs.

Ix

   b. In its purest sense, force protection is an overarching concept. It includes those procedural, training, equipment and leadership principles necessary to ensure the safety and well-being of our Marines, their family members, and our civilian employees. Force protection within the Marine Corps has its foundation in two tenets that have withstood time within our Corps, the first being that Marines take care of their own and the second being that commanders are ultimately responsible for the security of their personnel. In essence, force protection is an inherent function of command and as such should be an integral part of the way we do business on a daily basis.

4. <u>Relationship to Terrorism</u> Terrorism is defined as "the calculated use of violence or threat of violence to inculcate fear; its intended purpose is to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological." Combating terrorism encompasses aspects of antiterrorism (defensive measures which reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism) and is therefore an integral part of the overall force protection concept.

5. <u>Strategic Goal</u> The goal for the Marine Corps Antiterrorism/Force Protection Program is to protect our Marines, civilian employees, and family members from acts of terrorism and political turbulence. To this end, we must focus on those areas that we can best influence; such as the training and education of our Marines, proper operational planning, and the provision of the necessary resources to provide the best possible level of protection for our personnel. To meet this goal, the following objectives establish a proactive force protection program that provides the necessary awareness, training, equipment and resources:

   * Centers of Gravity. We must ensure that leaders at all
     levels understand the centers of gravity, both our's and
     the terrorist's. This is essential to the development of
     programs and the allocation of resources to reduce the
     threat to our personnel.

   * People. In order to combat terrorist threats we must
     inculcate a mindset of proactive planning as opposed to
     post-incident reaction. Key to developing this mindset
     is increasing the individual awareness of all personnel.

                                                              x

* Training and Education. While the foundation elements
  necessary to provide antiterrorism training to our
  personnel have been in place since the mid-l980s, we must
  implement measures to institutionalize training,
  particularly for deploying personnel.

* Operations. Force protection must be considered in all
  operational planning evolutions, to include the
  introduction of terrorist scenarios into our training
  exercises.

* Resources. Leaders must possess an understanding of the
  resources available to support force protection and an
  appreciation for the impact of intelligence analysis,
  security assessments, and budgeting in gaining the
  resources necessary to enhance organizational force
  protection efforts

6. <u>Understanding the Threat</u>

    a. The threat posed by the terrorist is fundamentally based
upon three supporting elements that may be viewed as a
three-legged stool. Each element1 or leg, supports the ability
of the terrorist to succeed in attacking our personnel and lends
stability to the terrorist's efforts. However, much like the
stool, when one leg is removed or altered, the stability is
reduced and the stool is likely to topple.
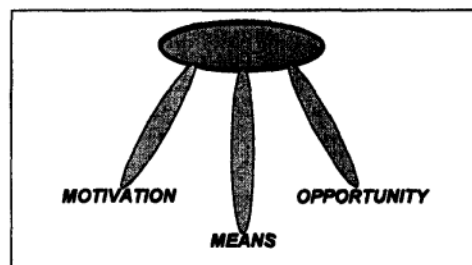
These elements are:

* Motivation: The willingness to strike against our
  personnel1 regardless of the difficulty presented by the
  target.

xi

* Means: The possession of, or ability to acquire, the
   resources necessary to carry out an attack against our
   forces.

* Opportunity: The ability to gain access to our personnel
   and facilities for the purpose of launching an act of
   terror.

   b. In a strategic sense, agencies outside the Marine Corps
have the best ability to influence motivation and means. The
factors which can reduce the terrorist's capabilities within
these elements encompass measures that go beyond the intent of
this Campaign Plan. However, for the Marine Corps to succeed in
its goal of ensuring force protection, we can and must minimize
the opportunity for the terrorist to target our forces. This can
best be done if we clearly understand the centers of gravity
which will enable us to reduce and minimize terrorist targeting.

7. <u>Supporting Functions</u> Key to our ability to enhance the
protection of our forces is reducing the terrorist's opportunity
to successfully strike at our personnel. In many respects this
may seem to be a formidable challenge given that the terrorist,
like a conventional enemy that has seized the initiative, chooses
the time and place of attack. However, like the conventional
enemy force, the terrorist can only attack those targets
presented him on his battlefield of terror. We can reduce the
opportunity for the terrorist to target our personnel and
minimize the chance of success by concentrating our efforts on
four supporting functions. They are:

* Intelligence

* Training and Education

* Operations

* Resources

CHAPTER 1

INTELLIGENCE

1001. GENERAL

1. The differences among tactical, operational, and strategic
levels of intelligence are principally ones of scope. Tactical
intelligence provides information on the environment and enemy
capabilities as they affect combat -- factors that have an
immediate or imminent impact. Operational intelligence provides
information which impacts on the campaign and therefore reflects
the broader perspective of operations. Operational intelligence
thus must take a wider view over area and a longer view over time
as the operational level of war is less a matter of actual
fighting and more a matter of schemes and intentions.
Operational intelligence focuses less on current combat
capabilities and more on forecasting future enemy capabilities,
intentions, and options.

2. Because the operational level of war has as its aim the
attainment of a strategic objective, operational intelligence
must provide insight into the strategic situation and all
factors, military and otherwise, that influence it. Most
information-gathering assets organic to the Commander must often
rely on assets external to the command for sources of operational
intelligence.

1002. ROLE OF INTELLIGENCE

1. As stated in MCDP 1-2 (Campaigning), intelligence is critical
to conducting any campaign. The role of intelligence in the
Marine Corps Antiterrorism/Force Protection Campaign Plan is no
less critical. The intelligence template for the sustainment of
the Marine Corps effort to combat terrorism and ensure the
protection of our forces is based on operational concepts.
Toward this end, intelligence must continue to ensure dedicated,
timely, and useful all-source analysis, production, and related
intelligence support which includes a continued focus on the
terrorist threat to Marine Corps personnel. A review of the
Marine Corps' multidisciplined intelligence capabilities focusing
on strategy, doctrine, policy, requirements, training,
resourcing, and planning will ensure success in our campaign to
protect our personnel.

2. From the strategic, operational and tactical perspective, intelligence priorities will include indications and warnings as well as terrorism threat analysis. This should be imbedded in doctrine, operational plans, and exercises and practiced religiously at every opportunity. The immediacy of terrorism and force protection information requires a communications architecture which supports the flow of intelligence throughout the chain of command and which maximizes the use of automated tools. The Marine Corps must have information connectivity that makes use of all available intelligence from all levels of intelligence database production elements. Achievement of the intelligence goal in the force protection arena will require developing a predictive intelligence capability. The standard order of battle intelligence has limited application against the terrorist threat. Identification of software packages which provide connectivity with national databases and permit link analysis at the lowest intelligence level is critical to the predictive analysis capability.

1003. <u>ROLE OF COUNTERINTELLIGENCE</u>

1. Counterintelligence support for antiterrorism and force protection efforts will continue to center on collecting threat information not obtainable through other collection platforms which the commander requires to carry out his responsibilities for protecting his personnel and equipment. Historically, counterintelligence has placed special emphasis on identifying terrorist threats to commands, specifically in the rear area, and will continue to do so in the future. Emphasis is placed on providing the commander with indications and warnings relating to the time, date, place, and method of attack as an integral part of the intelligence collection effort. Effective collection management at all levels focusing on the terrorist threat will reduce duplication of effort and ensure that the optimum collection resource is applied against the requirement.

2. Counterintelligence, along with law enforcement and other security elements, provide the commander with a means to conduct vulnerability assessments of the operating area. Vulnerability assessments assist the commander by identifying those physical and procedural security deficiencies which make the organization more susceptible to terrorist surveillance or attack.

1004. ANTITERRORISM/FORCE PROTECTION INTELLIGENCE OPERATIONS

1. To ensure the maximum benefit from intelligence resources,
Commanders must strive to enhance their capabilities.
Enhancement can be gained by considering the following:

> * Implementation of measures that facilitate the
>   multilateral exchange of intelligence information
>   when focusing on the terrorist threat. This
>   capability requires that dissemination procedures and
>   communications Systems be integrated into a seamless
>   system through the C4I/Global Command and Control
>   System (GCCS) concept. Operational commitments in
>   the coalition arena require training of, and improved
>   coordination with, allies in terrorism analysis,
>   collection, and reporting.
> * Institutionalization of antiterrorism/force
>   protection analysis during predeployment planning.
>   Antiterrorism/force protection plans must be an
>   integral component of every operation and exercise at
>   all levels of command.
> * Assessment of the effectiveness of intelligence
>   training programs, missions, equipment, and funding
>   through continual evaluations and oversight. In the
>   wake of increasing demands for intelligence and
>   counterintelligence resources to support force
>   protection efforts, periodic evaluation of the
>   adequacy of these resources within the tactical
>   structure must be undertaken.
> * Increased use of Marine Corps Reserve personnel
>   in intelligence analysis and the conduct of force
>   protection vulnerability assessments.

2. Effective application of intelligence to support this
campaign plan will reduce the vulnerability of our forces. The
concept requires a sustainable intelligence program to detect,
deter, and/or prevent terrorism through information superiority.
Our forward deployed forces serving as the principal means of
peacetime engagement, conflict prevention, and crisis response
will continue to be prime targets for the terrorist. To counter
this threat, properly focused and coordinated intelligence
resources are essential. It is not necessary to reinvent Marine
Corps intelligence to support our combating terrorism and force
protection effort. The key lies in expanding and shifting our
focus.

CHAPTER 2

TRAINING AND EDUCATION

2001. <u>GENERAL</u> Training and education are main factors in
reducing the terrorist's opportunity to target our forces.
Through training and education we increase the awareness level of
all personnel and reinforce that they can, in fact, become
victims of terrorism. Increasing awareness helps instill a
proactive mindset where each individual focuses on prevention of
terrorism rather than the post-incident response to a terrorist
attack. In essence, training and education are the cornerstones
to making antiterrorism/force protection a part of the way that
we do business on a daily basis.

2002. <u>DESIGNATION OF UNIT ANTITERRORISM/FORCE PROTECTION (AT/FP)
OFFICERS</u> Each Marine Corps unit of battalion/squadron size and
larger must designate an officer to serve as the unit AT/FP
Officer. Designation of a unit officer to fulfill this
responsibility is required by MCO 3302.1 and is essential to
ensuring that a viable training program is in place to provide
the necessary emphasis on AT/FP training and to properly prepare
our personnel to respond to terrorist threats. Officers assigned
to these duties must be provided the requisite training and
command support necessary to carry out their mission.

2003. <u>ANNUAL TRAINING REQUIREMENTS</u> MCO 3302.1_ requires that
all Marines receive antiterrorism training on an annual basis.
For most, this training is accomplished through the annual Marine
Battle Skills Test which incorporates training performance
standards pertaining to terrorism awareness and individual
protection measures. This training can be reinforced by
enrollment of personnel in the Marine Corps Institute Course
02.10b (Terrorism Awareness for Marines); the conduct of unit
level training using FMFM 7-14 (Combating Terrorism) and FMFRP
7-14A (The Individual's Guide to Understanding and Surviving
Terrorism); and through individual participation in
terrorism-based training exercises such as the annual terrorist
response exercise required by MCO 3302.1_. Integration of
terrorist scenarios into unit level training exercises provides
practical application of the skills taught in terrorism awareness
and serves to reinforce force protection readiness within the

unit. Accordingly, to the maximum extent possible, unit training exercises should incorporate scenarios that evaluate the unit's abilities to detect terrorist surveillance and targeting, to implement increased security measures as set forth for the various terrorist threat conditions (THREATCONs) set forth in MCO 3302.1_, and gauge the preparedness of the organization to respond to acts of terrorism as well as attack by traditional conventional enemy forces. The compendium of references in Appendix A provide useful sources of information that will assist in establishing and sustaining unit AT/FP training programs.

2004. <u>TRAINING FOR DEPLOYING PERSONNEL</u> Following the Khobar Towers bombing, the Chairman of the Joint Chiefs of Staff (CJCS) prescribed a four-level training program aimed at providing all deploying personnel an enhanced level of terrorism awareness. This training program requires that: a unit AT/FP officer be designated, that training be completed within six months prior to deployment, and that commanders certify that required training has been provided for all deploying personnel within six months prior to introduction of forces into a Combatant Commander's (CINCs) area of responsibility. Documentation of training in individual service member's records permits the commander to assess the current force protection readiness of his/her unit and ensures that, upon arrival in the operating area, personnel are prepared for any potential terrorist threat. The specific requirements of the four-level training program were set forth in CMC message 312020Z Jan 97 and will be incorporated into the next revision of MCO 3302.1_. The basics of this program are:

        * Level I (Individual Training) - Level I training
           focuses on the individual and forms the
           foundation of unit antiterrorism/force protection
           efforts. The emphasis is two fold -- to provide
           each individual with a basic understanding of
           terrorism and to improve personal protective
           measures. Through Level I training, each Marine
           will gain a better appreciation of the threat we
           face as they receive instruction on the history,
           motivation, organization, and tactics employed by
           terrorists and a theater-specific threat briefing
           for the region to which they will deploy.
           Hand-in-hand with this heightened awareness will
           be the refinement of individual protective
           measures. Instruction on detection of terrorist
           surveillance, hostage survival, actions to be

taken during leave, liberty and travel in foreign
countries, and similar training will enhance the
ability of our Marines to better protect
themselves. The intent of Level I training
is essentially to create a "hard target"
mentality among our personnel and to increase
both their awareness and their ability to
minimize the potential to become a victim of the
terrorist. The persona projected while
performing duties in a foreign land goes a long
way in thwarting the terrorist's opportunity.
Level I training will reinforce that every Marine
has a role in force protection and instill a
sense of personal responsibility.

* Level II (Unit AT/FP Officer Training) - As indicated
  in DoDD 2000.12H and DODI 2000.16, and incorporated in
  MCO 3302.1_, DOD/CJCS enhancement of force protection
  efforts include designation of a Unit AT/FP Officer at
  the battalion/squadron level and higher. The AT/FP
  Officer is responsible for establishment and management
  of the Level I training program. Additionally, the
  AT/FP Officer serves as an advisor to the commander on
  AT/FP issues. Although the Commander may call upon
  other staff officers for specific expertise on force
  protection matters (i.e., the S-2/CI Officer for threat
  information, S-4/Engineer Officer for barrier and
  obstacle planning, etc.), the designation of an AT/FP
  officer establishes a focal point for the gathering and
  dissemination of AT/FP information throughout the
  organization. Level II training provides the AT/FP
  Officer with the basic knowledge necessary to carry out
  these duties.

* Level III (Commander Training) - Inherent to
  command is the responsibility for the safety,
  security, and welfare of Marines, or in other
  words, their force protection. Commanders must
  prepare to meet the challenge of terrorism as it
  impacts on their ability to accomplish the
  mission. Our Commanders have the responsibility
  to understand their enemy's organizational
  structure, order of battle, tactics, and
  weaponry. This same ability is essential to

combating the terrorist. Level III training assists Commanders in transitioning their thought processes from conventional enemy forces to the terrorist. Level III provides an overview of DoD, CJCS, and Service guidelines regarding security standards, AT/FP objectives, and training requirements. Level III training is provided as an integral component of the Marine Corps Commanders Course held at Quantico, VA.

* Level IV (Executive Training) - Executive training is intended for personnel in the ranks of Colonel through Major General who have operational and planning responsibilities that encompass AT/FP issues. This training, hosted by the Deputy Director for Combating Terrorism (J-34), is conducted in seminar format that provides information on relevant terrorism and force protection topics and culminates with a computer aided antiterrorism wargame. Level IV training provides an opportunity to gain a better appreciation for the various agencies within our government that can provide intelligence and guidance when preparing for deployed operations as well as theater-specific information.

2005. SPECIALIZED TRAINING Certain Marines will be afforded specialized training based on the duties to which they are assigned. Additional information can be found in the annual Training Input Plan (TIP) published by Marine Corps Combat Development Command (MCCDC), Training and Education Division. Examples of specialized training include:

* Antiterrorism Instructor Qualification Course, Ft. Bragg, NC provides training for Unit AT/FP Officers, as well as intelligence, counterintelligence, and military police personnel who require the skills to conduct Level I training programs and implement installation antiterrorism programs.

* Individual Terrorism Awareness Course, Ft. Bragg, NC provides enhanced awareness training for personnel who routinely deploy to high threat areas or who are assigned to high risk billets.

* Combating Terrorism Aboard Military Installations, Ft. McClellan, AL provides military police instruction in law enforcement response to terrorist incidents occurring aboard DoD facilities.

* Dynamics of International Terrorism, Hurlburt Field, FL provides an overview of terrorist organizations and their methods of operation. This course provides a good introduction for personnel who are responsible for supervising antiterrorism programs.

* Conventional Physical Security Course, Ft. McClellan, AL provides training for military police personnel in evaluation of structural security, leading to assignment of secondary military occupational specialty 5814.

2006. <u>TROOP INFORMATION PROGRAM</u> An aggressive troop information program is key to ensuring that a constant level of terrorism awareness is maintained among our Marines and their family members. The Public Affairs Officer can play a significant role in supporting troop information efforts by incorporating awareness information such as travel security tips, articles on terrorism, training videos, etc. into the command's public affairs program. Additionally, innovative programs within the Command, such as the use of guest speakers and case studies, can greatly enhance awareness efforts.

CHAPTER 3

OPERATIONS

3001. <u>GENERAL</u> Force protection is an operational aspect of
every mission we undertake as Marines. Accordingly, Standing
Operating Procedures (SOPs), contingency plans, operations
orders, deployment plans, and after-action reports must take into
account antiterrorism/force protection issues. These documents
must consider the threat of terrorism, as well as the threat
posed to our forces by conventional enemy forces and must address
the actions that are to be taken in the event of a terrorist
incident. The challenge presented by terrorism is to develop
sound operational procedures that will enable the accomplishment
of the mission in a threat environment that may offer little or
no advance warning.

3002. <u>PASSIVE SECURITY MEASURES</u> Appropriate passive security
measures will do much to eliminate the belief that "opportunity"
exists. They include, but are not limited to, such items as
sound operational security (OPSEC) procedures, deception plans,
alternate routes, reconnaissance, and similar tactics employed
during conventional operations. In many instances, these
measures can be reinforced by incorporating passive security
systems that encompass the use of sensors, intrusion detection
devices, barriers, and obstacles. Regardless of the level of
technology employed, passive measures must be emphasized to the
point that they become second nature during operational planning
and mission execution. The mindset of every Marine must reflect
the vigilance that is required in the environment of terrorism.

3003. <u>THE VALUE OF ALARMS AND DRILLS</u> Commanders at every level
should develop recognizable alarms for potential emergencies and
critical incidents. They should create a means to immediately
sound the alarm and to develop reaction procedures that can be
tested with frequent drills. Repetitive performance of drills
will serve to familiarize all personnel with individual
responsibilities. Critical incident drills should be utilized to
exercise all phases of response. While more inherent to garrison
environment, attention should be given to unconventional tactics
employed by the terrorist. At a minimum drills should address
the indications and warnings process; associated Threat Condition
(THREATCON) security measures; preemptive evacuation procedures;
and mass casualty/medical responses.

3004. <u>RISK MANAGEMENT</u> The objective of the risk management process is the realistic identification of those assets that need or require protection, the risks to those assets based on a thorough assessment, and the security policies, practices and procedures that will provide the desired level of security at a price that we can afford. Achieving the objectives of the risk management process requires responsible and balanced thinking and decision making in developing, selecting, and implementing security policies, practices and procedures. We must be mindful that although the principles of managing risk are the same at all levels of government and industry, their application may differ as a result of differences in objectives, accountability mechanisms and legal requirements. The risk management process can be effective in situations where undesirable events could cause significant negative impacts and there are insufficient resources to defend against all such eventualities.

3005. <u>Readiness</u> Antiterrorism/force protection readiness has a direct impact upon the ability of the organization to successfully conduct its operations. In preparing for operations, the readiness of the unit must be assessed with regard to the ability to protect the force. In assessing antiterrorism/force protection readiness, factors to be considered include:

>   * The known or potential terrorist threat.
>   * Historical or demographic data regarding terrorism within the assigned area of operations.
>   * The level of antiterrorism training of the unit.
>   * The availability of additional resources to aid in minimizing the opportunity for terrorist targeting.
>   * The ability of the unit to respond if a terrorist attack occurs.

CHAPTER 4

RESOURCES

4001. <u>INFORMATION GATHERING</u>

1. In an effort to more effectively and efficiently utilize the
limited resources available, an accurate assessment of the threat
must be accomplished. Command assessments of the security
posture of the organization serve as a gauge of the adequacy of
resources. Assessment of vulnerabilities is a continual process.
Commanders should examine procedural areas, facilities, and
equipment resources where deficiencies could enhance terrorist
targeting. The vulnerability assessment parallels the
commander's estimate of the situation. A review of unit SOP,
operation/contingency plans, structural physical security
evaluations, and intelligence threat warnings and indicators all
serve to form the basis for a thorough assessment.

2. The terrorist threat assessment is a tool by which commanders
can arrive at a judgment of the risk and consequences of the
attack and balance the security effort and expenditures against
protection requirements. In conducting the assessment,
commanders should integrate threat information from the
intelligence community, technical information from security
planners and facilities engineers, and information from other
sources. A thorough threat assessment requires the collection of
all available information on terrorist activities. To that end,
intelligence assets inherent to the Marine Corps, as well as
information available from the Navy's Antiterrorism Alert Center
(ATAC) and other Services/agencies should be utilized to the
maximum extent possible. In doing so, the commander gains a
broader perspective of physical security, security engineering,
and operational activities that must be addressed in order to
successfully avoid, deter, or mitigate terrorist attacks. Once
completed, the threat assessment provides the basis and
justification for recommendations regarding force protection
enhancements and program/budget requests.

3. The Marine Corps program for evaluating security programs and
assessing vulnerability is accomplished by using several levels
of evaluations. Physical security specialists assigned to each
installation Provost Marshal Office conduct annual physical

security evaluations of those key facilities aboard the
installation that the Commander has determined to be critical to
mission performance, such as arms, ammunition and explosive
(AA&E) storage areas, command headquarters facilities and
Classified Material Control Centers. Likewise, organic
counterintelligence personnel conduct vulnerability assessments,
in conjunction with Naval Criminal Investigative Service
personnel, for Marine Corps activities to gauge threats posed by
terrorist groups and to identify weaknesses in the information
and operational security arena. Personnel from HQMC and from the
Naval Surface Warfare Center, Crane, IN conduct site visits
independently to assess installation facilities. The Inspector
General of the Marine Corps assesses the functional areas of
physical security and antiterrorism during the review of
Commanding General's Inspection Programs at each installation and
select Unit Inspection Programs. Finally, the Defense Special
Weapons Agency (DSWA) has been tasked by CJCS to assess the
vulnerability of DoD activities and will periodically review
designated Marine Corps bases.

4002. <u>PROGRAMMING RESOURCES</u>

1. The commander's assessment of the force protection posture of
the organization is critical to ensuring that resource
deficiencies are addressed so that follow-on action can be taken
to provide the necessary funding and equipment to overcome any
shortfalls. Deficiencies in the security program will normally
be identified during internal and external assessments. While
some deficiencies may be correctable through modification to
local procedures and the realignment of existing resources,
others will require dedicated funding for procurement of
equipment, construction of facilities, and enhancement of
training. Security deficiencies, as well as force protection
enhancements, must be identified and validated as requirements.

2. To assist commanders, HQMC (POS) programs funds for physical
security upgrade projects for sensitive facilities such as AA&E
sites. Commanders can request funds by submitting a Fleet
Operational Needs Statement (FONS) to the program sponsor (POS).
Commanders should also consider submitting a Program Objectives
Memorandum (POM) initiative during their POM development process.

4-2

The program will then compete against other initiatives during POM prioritization. Additionally, the Secretary of Defense has established a Combating Terrorism Readiness Initiatives Fund (CbTRIF). The CbTRIF, managed by CJCS, provides dedicated funding to support force protection enhancements for the CINCs and their assigned operating forces. Requests must be for unanticipated requirements whose funding urgency cannot be met through the normal Service funding process. Additional information concerning the CbTRIF can be found in CJCSI 5261.01.

CHAPTER 5

COMMANDER'S RESPONSIBILITY

5001. <u>GENERAL</u> Preventive and protective security measures should be taken by military units and individual Marines to protect themselves and their ability to accomplish the mission during deployment and expeditionary operations. The degree of antiterrorism/force protection measures taken depends on the threat in a given location. Commanders must constantly evaluate security against the terrorist threat in order to effectively determine security requirements.

5002. <u>COMMANDER'S ESTIMATE</u> The commander1s estimate of the vulnerability of his unit to terrorist acts forms the basis for implementation of force protection measures. The commander and his staff should complete a thorough estimate of the terrorist situation using mission, enemy, terrain, troop-time. The Commander's Estimate of the Situation at Appendix B will assist in assessing the vulnerability of the operating area in the event that dedicated resources are not available to conduct a formal assessment.

5003. <u>COMBATING TERRORISM PROGRAM STANDARDS</u> The DoD Combating Terrorism Program Standards are provided at Appendix C. These performance-based standards form the baseline for the execution of combating terrorism policy and the foundation necessary to implement a comprehensive antiterrorism/force protection (AT/FP) program. These standards address the full spectrum of AT/FP requirements, including AT/FP threat assessment and threat information flow, AT/FP planning and program implementation, vulnerability assessments, and training requirements. Implementation of the standards at the installation and unit (battalion/squadron and higher) level will serve to enhance the protection of our Marines and Sailors, their families, our civilian employees and facilities.

ANTITERRORISM/FORCE PROTECTION CAMPAIGN PLAN

APPENDIX A

COMPENDIUM OF REFERENCES

The following references are not all inclusive and are provided
as a basis for additional information that may assist in force
protection efforts.

A. DEPARTMENT OF DEFENSE

    * DoD Directive 1300.7 of 23 Dec 88 (Training and Education
       Measures Necessary to Support the Code of Conduct)

    * DoD Directive 2000.12 of 15 Sept 96 (DoD Combating
       Terrorism Program)

    * DoD Directive 0-2000.12H of XX XXX 97 (Protection of
       Department of Defense Personnel and Assets Against Acts of
       Terrorism and Political Turbulence)

    * DoD Instruction 2000.16 of 21 Jul 97 (DoD Combating
       Terrorism Program Standards)

    * DoD Directive 3025.14 of 5 Nov 90 w/changes (Protection
       and Evacuation of U.S. Citizens and Designated Aliens in
       Danger Areas Abroad - (Short Title: Noncombatant Evacuation
       Operations)

    * DoD Directive 5200.8-R of 13 May 91 (DoD Physical Security
       Program)

    * DoD Directive 5210.84 of 22 Jan 92 (Security of DoD
       Personnel at U.S. Missions Abroad, Enclosure 1, Memorandum
       of Understanding Between DoD and DoS on Overseas Security
       Support)

    * DOD Directive 5240.1 of 25 Apr 88 (DoD Intelligence
       Activities)

    * DoD Directive 5240.1-R of Dec 82 (Procedures Governing the
       Activities of DoD Intelligence Components That Affect
       United States Persons) [as authorized by DoD Directive
       5240.1 of 25 Apr 88]

* DoD Directive 5240.6 of 26 Feb 86 (Counterintelligence
  Awareness and Briefing Program)

* DoD Instruction 3020.27 of 6 Nov 90 w/change (Continuation
  of Essential DoD Contractor Services During Crisis)

* Department of Defense and Department of State Memorandum
  of Understanding on Force Protection of 15 Sep 96

B. JOINT PUBLICATIONS

* Joint Pub 2-01 (Joint Intelligence Support to Operations)

* Joint Pub 2-02 (National Intelligence Support to Joint
  Operations)

* Joint Pub 3-0 (Doctrine for Joint Operations)

* Joint Pub 3-05 (Doctrine for Joint Special Operations)

* Joint Pub 3-05.3 (Joint Special Operations Operational
  Procedures)

* Joint Pub 3-54 (Joint Doctrine for Operations Security)

* Joint Pub 3-07.2 (Joint Tactics, Techniques, and
  Procedures for Antiterrorism)

* Joint Pub 3-07 (Joint Doctrine for Military Operations
  Other Than War)

* Joint Pub 3-10.1 (Joint Tactics, Techniques, and
  Procedures for Base Defense)

* Joint Pub 5-03.2 (Joint Operations Planning and Execution
  System, Volume II (Planning and Execution Formats and
  Guidance)

* Joint Staff Guide 5260 (Service Member's Personal
  Protection Guide: A Self-Help Handbook to Combating
  Terrorism)

ANTITERRORISM/FORCE PROTECTION CAMPAIGN PLAN

C.   DEPARTMENT OF THE NAVY

   *   SECNAVINST 3300.2 of 9 Jan 92 (Combating Terrorism
       Program)

   *   SECNAVINST 3820.3 of 24 Aug 88 (Oversight of Intelligence
       Activities within the Department of the Navy)

   *   SECNAVINST 3875.1 of 2 Nov 88 (Counterintelligence and
       Awareness Briefing Program)

   *   SECNAVINST 4862.10 of 5 Nov 90 (DoD Key Asset Protection
       Program)

   *   SECNAVINST 5500.34 of 15 Sep 92 (Security of DoD
       Personnel at U.S. Missions Abroad)

   *   OPNAVINST 3300.53 of 1 May 92 (Navy Combating Terrorism
       Program)

   *   OPNAVINST 3300.54 of 3 Aug 93 (Protection of Navy
       Personnel and Activities Against Acts of Terrorism and
       Political Turbulence)

   *   OPNAVINST 5530.13 of 5 Jul 95 (DoN Physical Security
       Instruction for Conventional Arms, Ammunition, and
       Explosives)

   *   OPNAVINST 5530.14 of 21 Dec 88 (DON Physical Security and
       Loss Prevention Manual)

   *   Commander Naval Education and Training Center Directive
       5530.2 of 17 Mar 95 (Physical Security, Loss Prevention,
       Antiterrorism, and Naval Security Forces Ashore Program)

   *   Naval Civil Engineering Laboratory, Port Hueneme, CA
       (Terrorist Vehicle Bomb Survivability Manual, July 1988)

D.   UNITED STATES MARINE CORPS

   *   FMFM 7-14 (Combating Terrorism)

   *   FMFRP 7-14A (The Individual's Guide to Understanding and
       Surviving Terrorism)

* FMFRP 7-37 (Vehicle Bomb Search)

* MCO 1510.89 (The Individual Training Standards (ITS) System for Marine Battle Skills Training (MBST); MBST Handbook 1 (General Military Subjects)

* MCO 3302.1B (The Marine Corps Antiterrorism Program)

* MCO 5500.13 (Physical Security)

* MCO 5500.14A (Flight Line Security)

* MCO 5500.18 (Crime Prevention)

* MCO 5580.2 (Marine Corps Law Enforcement Manual)

* MCI Course 02.1Db (Terrorism Awareness for Marines)

E. MISCELLANEOUS

* Public Law 99-399 of 27 Aug 86 as amended (Omnibus Diplomatic Security and Antiterrorism Act of 1986)

* Department of State Publication DOS-2630-48-82 (Handbook on Terrorism, Security, and Survival)

* Department of the Army Field Manual FM 19-30 (Physical Security)

* Department of the Army Field Manual FM 100-37 (Terrorism Counteraction)

* Department of the Army Training Circular TC 19-16 (Countering Terrorism on U.S. Army Installations)

ANTITERRORISM/FORCE PROTECTION CAMPAIGN PLAN

APPENDIX B

COMMANDER'S ESTIMATE OF THE SITUATION

A. MISSION:

    1. Who is being tasked?

    2. What is the task and why are we performing it?

    3. When and where is this task to be performed?

B. ENEMY:

    1. Who are the potential terrorists?

    2. What is known about the terrorists?

    3. How do the terrorists receive information?

    4. How might the terrorists attack? (As seen from the
        terrorist's view)

    5. Does your unit have routines?

    6. What is the potential for civil disturbances and could
        terrorists use/influence these to facilitate an attack?

C. TERRAIN:

    1. What are the strengths and weaknesses of the
        base, operating area, and local surroundings?

    2. Are there avenues of approach that could be exploited by
        terrorists?

    3. Are there observation areas, dead spaces, fields of
        fire, illumination, or no-fire areas?

    4. Are there tall buildings, water towers, or terrain
        either exterior or adjacent to the perimeter that could
        become critical terrain in the event of an attack?

D.   TROOPS:

    1.   What is the friendly situation?

    2.   Are there other U.S. forces or equipment available?

    3.   Are engineers in the area? Will they be able to
       provide support?

    4.   Are emergency reinforcements available?

    5.   Are military working dog teams available?

    6.   What are the host nation responsibilities,
       capabilities, and attitudes toward providing
       assistance?

    7.   What restraints will be imposed by the U.S. Government
       on the show or use of force?

    8.   If the situation deteriorates, what are the criteria for
       withdrawing troops from the area and what provisions
       are in place for marshaling and evacuating personnel?

E.   TIME:

    1.   What is the duration of the mission?

    2.   Are there time constraints?

    3.   Will there be sufficient time to construct force
       protection facilities such as weapons/fighting
       positions, barriers, obstacles, fences, and lights?

F.   POLITICAL PLANNING FACTORS:

    1.   Are there host nation concerns or attitudes that will
       impact on the situation?

    2.   Will the situation be influenced by the existence of
       any religious or racial concerns?